What is claimed is:

1. A method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of:

encrypting the original document with a unique session key to create an encrypted document;

generating a proxy key based on a public key corresponding to the selected recipient; and

transforming the encrypted document with the proxy key to create a transformed document.

2. The method of claim 1, further comprising the step of transmitting the transformed document to the selected recipient.

3. The method of claim 1, further comprising the steps of:

recovering the unique session key from the transformed document; and

decrypting the transformed document with the session key to recover the original document.

4. The method of claim 3, wherein the recovering step is performed by applying a private key corresponding to the selected recipient.

5. The method of claim 1, wherein the encrypting step is performed with a symmetric private-key encryption scheme.

6. The method of claim 5, wherein the encryption scheme is based on the ElGamal cryptosystem.

7. The method of claim 5, wherein the encrypted document comprises a first portion representative of the original document encrypted via the symmetric private-key

encryption scheme using the session key, and a second portion representative of the session key encrypted using an owner's private key.

8. The method of claim 1, wherein the original document is distributed to the selected recipient through at least one additional intermediate grantor by repeating the generating and transforming steps for each additional intermediate grantor.